CLAIMS:

1. A method of providing to a client communications device access to a subscription module of a server communications device, the method comprising the steps of

- establishing (301) a communications link between the client communications device (300) and the server communications device (310); and
- communicating (304;403,404) a number of messages (M) comprising data related to the subscription module (318) between the server communications device and the client communications device via the communications link;

characterised in that

the method further comprises the step of providing (402,405) integrity protection of the messages communicated between the server communications device and the client communications device via the communications link.

2. A method according to claim 1, characterised in that the step of providing integrity protection further comprises calculating, based on a secret session key, a respective message authentication code for each of the communicated messages; and including the calculated message authentication code into the corresponding communicated message.

3. A method according to claim 2, characterised in that the step of establishing a communications link between the client and server communications devices comprises determining a secret session key based on a shared secret between the server and client communications devices.

4. A method according to claim 3, characterised in that the method further comprises providing the shared secret by performing a secure pairing

procedure including receiving a passcode by at least one of the client communications device and the server communications device.

5. A method according to claim 4, characterised in that the passcode is at the most 48 bits long.

6. A method according to claim 3, characterised in that the communications link has a secret link key related to it and the method further comprises providing the shared secret by calculating the shared secret using the secret link key as an input.

7. A method according to any one of claims 2 through 6, characterised in that the method further comprises

- incorporating a value of a first counter in each of the messages communicated from the client communications device to the server communications device, the first counter being indicative of the number of messages communicated from the client communications device to the server communications device; and
- incorporating a value of a second counter in each of the messages communicated from the server communications device to the client communications device, the second counter being indicative of the number of messages communicated from the server communications device to the client communications device;

and the step of calculating a respective message authentication code for each of the communicated messages comprises calculating a message authentication code for each of the communicated messages and the corresponding counter value.

8. A method according to any one of claims 1 through 7 characterised in that the method further comprises determining, for the messages communicated from the client communications device to the server communications device, whether the message is authorised to address the subscription module.

9. A method according to claim 8, characterised in that the method further comprises providing a shared secret between the client communications device and the server communications device; and providing an access control list stored in the server communications device in relation to at least one of the shared secret and the client communications device.

10. A communications system comprising a client communications device (106,206) and a server communications device (101,201) including a subscription module(102;202), the client and server communications devices each comprising respective communications means (110,104;204,210) for establishing a communications link (115) between the client communications device and the server communications device, and for communicating a number of messages comprising data related to the subscription module between the server communications device and the client communications device via the communications link;

characterised in that

the client communications device and the server communications device each comprise respective processing means (105,107;203,209) adapted to provide integrity protection of the messages communicated between the server communications device and the client communications device via the communications link.

11. A server communications device including a subscription module, the server communications device comprising communications means for establishing a communications link with a client communications device, and for communicating a number of messages comprising data related to the subscription module between the server communications device and the client communications device via the communications link;

characterised in that

the server communications device comprises processing means adapted to provide integrity protection of the messages communicated between the server communications device and the client communications device via the communications link.

12. A client communications device for providing access to a subscription module of a server communications device, the client communications device comprising communications means for establishing a communications link with the server communications device including the subscription module, and for communicating a number of messages comprising data related to the subscription module between the client communications device and the server communications device via the communications link;

characterised in that

the client communications device comprises processing means adapted to provide integrity protection of the messages communicated between the client communications device and the server communications device via the communications link.

13. A method of providing to a client communications device access to a subscription module by a server communications device comprising the subscription module, the method comprising the steps of

- establishing (301) a communications link between the client communications device (300) and the server communications device (310) ; and
- receiving (404) a number of messages from the client communications device by the server communications device via the communications link, the messages addressing the subscription module (318);

characterised in that

the method further comprises the step of determining (701), for at least one of the received messages, whether the message is authorised to address the subscription module.

14. A method according to claim 13, characterised in that the method further comprises providing integrity protection of the messages communicated between the server communications device and the client communications device via the communications link, where the integrity protection is based on a shared secret between the client communications device and the server communications device; and providing an access control list stored in the server communications device in relation to at least one of the shared secret and the client communications device.

15. A method according to claim 14, characterised in that the access control list is stored in a protected database.

16. A method according to claim 14 or 15, characterised in that the method further comprises calculating, based on a secret session key, a respective message authentication code for each of the communicated messages; and including the calculated message authentication code into the corresponding communicated message.

17. A method according to claim 16, characterised in that the step of establishing a communications link between the client and server communications devices comprises determining the secret session key based on said shared secret between the server and client communications devices.

18. A method according to claim 17, characterised in that the method further comprises providing the shared secret by performing a secure pairing procedure including receiving a passcode by at least one of the client communications device and the server communications device.

19. A method according to claim 18, characterised in that the passcode is at the most 48 bits long.

20. A method according to claim 18, characterised in that the communications link has a secret link key related to it and the method further comprises providing the shared secret by calculating the shared secret using the secret link key as an input.

21. A method according to any one of claims 14 through 20, characterised in that the method further comprises

- incorporating a value of a first counter in each of the messages communicated from the client communications device to the server communications device, the first counter being indicative of the number of messages communicated from the client communications device to the server communications device; and
- incorporating a value of a second counter in each of the messages communicated from the server communications device to the client communications device, the second counter being indicative of the number of messages communicated from the server communications device to the client communications device;

and the step of calculating a respective message authentication code for each of the communicated messages comprises calculating a message authentication code for each of the communicated messages and the corresponding counter value.

22. A server communications device including a subscription module, the server communications device comprising communications means for establishing a communications link with a client communications device, and for receiving a number of messages addressing the subscription module from the client communications device via the communications link;

characterised in that

the server communications device comprises processing means for determining, for at least one of the received messages, whether the message is authorised to address the subscription module.